The overall objective is to provide an easily accessible and useful source of information to Federal employees on effective security tools and practices.

John Gilligan
Former CIO, Dept. of Energy &
Chair, CIO Council Security Subcommittee

Agencies' sharing of successful BSPs helps bridge from "what should be done" to "what is being done" for effective IT security.

Marianne Swanson
National Institute for Standards and Technology &
Chair, Federal Computer Security Managers Forum

The Agency's BSPs are beginning to be used by developing nations seeking an effective model for their own cyber security. This places the United States and USAID in a leadership role.

Peter Benedict
CIO, US Agency for International Development

BSPs provide all Federal IT professionals with up-to-date and inexpensive information security know how… BSPs can be freely shared, used, improved, and reused.

Jim Craft, CISSP
ISSO, US Agency for International Development
Chair, CIO Council Security Practices Subcommittee

A Role for Everyone

Practitioners know first-hand their practices worthy of sharing.

Agency managers provide the supportive environment essential for successful information sharing.

CIOs and the CIO Council provide the institutional leadership and the website's technical capability.

Service and solution vendors often provide the mechanisms and tools which enable practices to succeed.

Federal Best Security Practices

http://bsp.cio.gov

For further information contact:

National Institute for Standards and Technology (NIST)
Marianne Swanson
301.975.3293
marianne.swanson@nist.gov

General Services Administration (GSA)
Keith Thurston
202.501.3175
keith.thurston@gsa.gov

National Security Agency (NSA)
Mary Schanken
410.854.4458
schanken@nsa.gov

Chair, Security Practices Subcommittee
Jim Craft, CISSP
US Agency for International Development (USAID)
202.712.5460
jcraft@usaid.gov

Best Security Practices (BSPs) Are Important

- Decrease reinvent-the-wheel frustration
- Decrease the likelihood of unsuccessful results
- Increase accuracy of cost estimates
- Identify faster solutions
- Earn professional and organizational recognition

BSPs are Easy to Find

- Use simple key word search
- Sort by security process area (see below)
- View other users' feedback

BSPs are Available in These Security Process Areas

- Security Program Management
- Personnel Security
- Security Training
- Physical Security
- Contingency Planning
- Technical Security
- Incident Response
- Risk Management
- Certification & Accreditation
- Customer Security Support

BSPs Are:

- A human activity
- Security-related
- Existing practices
- Shown effective by experience
- Among the most effective

BSPs are Not:

- IT security tools
- Business practices
- The best possible practices
- Necessarily the single best

The BSP Format is Straightforward

- BSP identification and POC information
- Background
- Description of inputs, process, and outputs including actual artifacts
- Implementation lessons learned and performance measures
- Appendices for briefings, vendor or product procurement information, references, etc.

It's Simple to Submit a BSP

- Download and complete template
- Request informal review (see POCs on back page of this flyer)
- Gain organizational approval to submit… usually your ISSO or IRM
- Click <Submit> w/ email attachments

How are BSPs Evaluated?

- All BSPs are reviewed by GSA and NIST for editorial content and to validate the submitter's identity before public posting.
- Once posted, any user may submit feedback on a particular BSP.
- Utilization and user feedback are the primary methods to determine BSP quality.
- User feedback also provides information to BSP submitters to help improve a particular BSP.

http://bsp.cio.gov